Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1. (Original) A method for operating a portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising the steps of:

coupling the portable authorization device to the host system;

receiving a first item of authorization information from a first type of information authority;

receiving a second item of authorization information from a second type of information authority; and

selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information.

2. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a first interface operative in conjunction with the processing unit and the storage medium for receiving a first item of authorization information from a first type of

information authority;

a second interface operative in conjunction with the processing unit and the storage medium for receiving a second item of authorization information from a second type of information authority; and

a third interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information;

wherein the portable authorization device is removably couplable to the host system through the third interface.

3. (Original) The portable authorization device of claim 2, wherein:

the first interface comprises a direct information authority interface program;

the first type of information authority comprises a direct information authority operatively coupled directly to the portable authorization device;

the second and third interfaces each comprise a same host system interface program; and

the second type of information authority comprises an indirect information authority operatively coupled to the portable authorization device through the host system.

4. (Original) The portable authorization device of claim 3, wherein the indirect

information authority comprises a computer system coupled to the host system via a network.

5. (Original) The portable authorization device of claim 3, wherein the indirect information authority comprises data stored on a magnetic storage medium.

6. (Original) The portable authorization device of claim 2, further comprising:

a host authorizer operative in conjunction with the processing unit and the third interface for selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information.

7. (Original) The portable authorization device of claim 6, wherein the host authorizer is a software program operatively stored in the storage unit.

8. (Original) The portable authorization device of claim 6, wherein:

the first and second items of authorization information comprise first and second key selectors, respectively; and

the host authorizer in conjunction with the processing unit and the third interface operatively generates a key based upon the first or second key selectors and selectively authorizes the host system to use the one or more items of protected information based upon the key.

9. (Original) The portable authorization device of claim 2, wherein the first interface is configured to conduct a challenge-response transaction with the first type of information authority.

10. (Original) The portable authorization device of claim 2, wherein the second interface is configured to conduct a challenge-response transaction with the second type of information authority.

11. (Original) The portable authorization device of claim 2, wherein the third interface is configured to conduct a challenge-response transaction with the host system.

12. (Original) An authorization system for selectively authorizing a host system to use one or more items of protected information, comprising:

an access control mechanism associated with the host system for receiving a first item of authorization information from a first type of information authority operatively coupled to the host system and for forwarding the item of authorization information to the portable authorization device; and

a portable authorization device removably couplable to the host system for receiving the first item of authorization information from the access control mechanism and for selectively authorizing the host system to use the one or more items of protected information based upon the first item of authorization information.

13. (Original) The authorization system of claim 12, wherein:

the portable authorization device is configured to also receive a second item of authorization information from a second type of information authority operatively coupled to the portable authorization device and, furthermore, is configured to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information.

14. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a first interface operative in conjunction with the processing unit and the storage medium for receiving a key selector from an information authority;

a host authorizer operative in conjunction with the processing unit and the storage medium for generating a key based upon the key selector; and

a second interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the key;

wherein the portable authorization device is removably couplable to the host system through the second interface.

15. (Original) The portable authorization device of claim 14, wherein:

the first interface comprises an information authority interface; and

the second interface comprises a host system interface.

16. (Original) A portable authorization device for selectively authorizing a host system to use a plurality of items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit for storing one or more items of blended authorization information, each item of blended authorization information being derived from a plurality of items of authorization information;

an unblending mechanism operative in conjunction with the processing unit and the storage medium for regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information; and

a host system interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information;

wherein the portable authorization device is removably couplable to the host system through the host system interface.

17. (Original) The portable authorization device of claim 16, wherein:

each item of blended authorization information is derived from the two or more items of authorization information by performing an arithmetic operation on the two or more items of authorization information.

18. (Original) A method for operating a portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising the steps of:

coupling the portable authorization device to the host system;

receiving a plurality of items of authorization information;

generating one or more items of blended authorization information from the plurality of items of authorization information;

storing the one or more items of blended authorization information in a storage medium;

retrieving one or more of the items of blended authorization information from the storage medium;

regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information; and

selectively authorizing the host system to use an item of protected information based upon the at least one item of authorization information.

19. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a first storage medium operatively coupled to the processing unit for storing one or more encoded items of authorization information;

a second storage medium operatively coupled to the processing unit for storing decoding information used to decode the one or more encoded items of authorization information, wherein the second storage medium is accessible by the processing unit only if the processing unit receives proper authorization;

a decoding mechanism operative in conjunction with the processing unit and the first and second storage media for decoding at least one of the one or more encoded items of authorization information to produce at least one respective item of authorization information; and

an interface operative in conjunction with the processing unit for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information.

20. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a first storage medium operatively coupled to the processing unit for storing one or more encoded items of authorization information;

a second storage medium operatively coupled to the processing unit for storing a plurality of items of decoding information;

a decoding mechanism operative in conjunction with the processing unit and the first and second storage media for decoding at least one of the one or more encoded items of authorization information using a selected one of the plurality of items of decoding information to produce at least one respective item of authorization information; and

an interface operative in conjunction with the processing unit for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information.

21. (Original) A portable authorization device, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a first interface operative in conjunction with the processing unit and the storage medium for receiving a first item of information from a first information authority; and

a second interface operative in conjunction with the processing unit and the storage medium for transmitting a second item of information to a second information authority.

22. (Original) The portable authorization device of claim 21, wherein:

the first item of information comprises an item of authorization information for selectively authorizing a host system to use one or more items of protected

information;

the second item of information is the same as the first item of information; and

the portable authorization device disables or removes the item of authorization information from therein upon transmission to the second information authority.

23. (Original) The portable authorization device of claim 22, wherein the second information authority is a second portable authorization device.

24. (Original) A portable authorization device, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a message manager operative in conjunction with the processing unit and the storage medium for determining whether the portable authorization device is authorized to receive an item of authorization information from an information authority; and

an interface operative in conjunction with the processing unit, the storage medium and the message manager for receiving the item of authorization information from the information authority if the portable authorization device is authorized to receive the item of authorization information.

25. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit for storing an enable field and a counter associated with a set of items of protected information; and

an interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use a subset of the set of items of protected information based upon values of both the enable field and the counter.

26. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a password manager operative in conjunction with the processing unit and the storage medium for determining if a predetermined password authorization condition is satisfied with respect to the host system and if not, obtaining and verifying a password entered by a user; and

an interface operative in conjunction with the processing unit, the storage medium and the password manager for communicating with the host system to selectively authorize the host system to use the one or more items of protected information only if the predetermined password authorization condition is satisfied.

27. (Original) A system for reconstructing a portable authorization device,

comprising:

a portable authorization device that operatively stores one or more items of authorization information for selectively authorizing a host system to use one or more items of protected information; and

reconstruction data disposed on the host system for reconstructing the items of authorization information operatively stored in the portable authorization device.

28. (New) A portable security device removably coupled to a computer system for selectively authorizing the computer system to use multiple items of protected information, comprising:

a processing unit;

at least one storage medium coupled to the processing unit;

an interface capable of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within the at least one memory; and

an interface program for selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

29. (New) The method of claim 28 wherein the multiple items of authorization information comprise key selectors.

30. (New) The method of claim 29 a key is generated within the portable security device based upon the key selectors and selective authorization is given to the computer system to use the multiple items of protected information based upon the key.

31. (New) The method of claim 28 wherein the multiple items of authorization information comprise one or more secret keys.

32. (New) The method for selectively authorizing the use of multiple items of protected information on a computer system using a portable security device that is removably coupled to the computer system, the method comprising the steps of:

(a) providing the portable security device with the capability of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within a single memory in the portable security device; and

(b) selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

33. (New) The method of claim 32 wherein the multiple items of authorization information comprise key selectors.

34. (New) The method of claim 33 further including the step of: generating a key within the portable security device based upon the key selectors and selectively authorizing the computer system to use the multiple items of protected information based upon the key.

35. (New) The method of claim 32 wherein the multiple items of authorization information comprise one or more secret keys.

36. (New) A method for selectively authorizing the use of multiple items of protected information on a computer system, the method comprising the steps of:

(a) providing a portable security device with at least one memory containing a shared secret and space for multiple key selectors, one key selector for each item of protected information, and at least one I/O port, whereby the key selectors can be downloaded into the security device, and communications can be established with the computer system;

(b) receiving by the portable security device an authorization request from the computer system to authorize use of a particular one of the items of protected information; and

(c) using the stored key selector corresponding to the particular one of the items and the shared secret to generate authorizing information, wherein the computer system validates the authorizing information and releases the particular one of the items of protected information for use.

37. (New) The method of claim 36 further including the step of providing the key selectors to the portable security device memory using external information authorities within a secure transaction.

38. (New) The method of claim 37 further including the step of receiving a random challenge from the information authority, using the shared secret to encrypt the response, and validating by the information authority the response by decrypting with the shared secret.

39. (New) The method of claim 36 where the shared secret is an encryption key.

40. (New) The method of claim 39 further including the step of transforming the received key selector into an authorizing key using the shared secret key.

41. (New) The method of claim 40 where the authorization request is a randomly generated challenge number.

42. (New) The method of claim 41 where the authorization information is generated by using the challenge and the authorizing key.

43. (New) The method of claim 36 further including the step of encrypting the key selectors before storing in the portable security device memory.

44. (New) The method of claim 43 further including the step of storing the key selectors in a merged pool in memory using a blending algorithm, whereby an individual key selector cannot be extracted from a specific location in memory.

45. (New) The method of claim 36 further including the step of receiving the multiple items of information from multiple information authorities.